



Subject	Date Last Reviewed	Policy #
Physical Facilities Access Policy	November 2021	ENG-1.0
	Application	Supersedes
	Facilities	
	Distribution	
	All Departments	
Recommended	Approved	
 Kenny Stansfield, Director of Facilities Management	 Preston D. Marx, VP Information Systems	

Physical Facility Access Policy

1. Overview

Administration, managers, plant operations staff, human resources, and information technology are responsible for facility access requirements. The management and monitoring of physical access to facilities is extremely important to Uintah Basin Healthcare(UBH) security, patient safety and helps maintain information as well.

2. Purpose

This policy establishes rules for management, control, monitoring, and removal of physical access to UBH facilities.

3. Scope

This policy applies to all UBH staff.

4. Policy

A. GENERAL

Physical access to all restricted facilities shall be documented and managed. All facilities must be physically protected relative to the criticality or importance of the function or purpose of the area managed.

Requests for access shall come from the applicable manager in the area where the access is requested. Access to facilities will be granted only to personnel whose job responsibilities require access. Electronic access control systems shall be used to manage access to

controlled spaces and facilities.

The process for granting card and/or key access resides with UBH human resources and plant operations. Human resource department will create new badges for employees and upon assigning a department and title with user will be given the default access for that position. All requests for further access must be recorded by requests through the TMA Engineering Request System by the appropriate department manager and will then be managed by the plant operations manager or designee. They shall regularly review card and/or key access rights and remove access for individuals that no longer require access or persons who leave UBH. Access rights shall be based on an employee's (staff, visitor, contractor, etc.) role or function in the organization.

B. MANAGEMENT RESPONSIBILITIES

The plant operations manager or their designee shall ensure:

- Secure areas are protected by appropriate entry and controls for authorized personnel
- Procedure's control and validate a staff member's access to facilities with the use of security personnel, identification badges, or electronic key cards
- Procedures exist that establish visitor controls including visitor sign-in logs and wearing of visitor badges for both entry and exit of UBH
- Policies specify management's review of the list of individuals with physical access to facilities containing sensitive information (whether in paper or electronic forms)
- Card access records and visitor logs for facilities are kept for periodic review based upon the security requirements of the location

C. KEY ACCESS AND CARD SYSTEMS

The following policy applies to all facility access cards/keys:

- Employee access cards and/or keys must not be shared or loaned to others
- Access cards/keys shall not have identified information other than a return mail address and all cards/keys that are no longer required must be returned to UBH human resources
- Lost or stolen cards/or keys must be reported immediately UBH human resources
- UBH human resources shall remove card and/or key access rights of individuals that change roles or are separated from their relationship with UBH
- The plant operations manager or their designee regularly reviews access records and visitor logs for the facility and is responsible for investigating any unusual events or incidents related to physical facility access

D. SUB CONTRACTOR AND GUEST ACCESS

The following policy and procedure apply to identification and authorization of sub-contractor and guests to UBH:

- Visitors shall be identified and given a badge or other identification identifies them as a sub-contractor or guest
- Visitors shall surrender the badge or identification before leaving the facility or at the date of expiration
- Visitors shall be authorized before entering, and escorted at all times within, areas that are sensitive or patient safety is necessary
- Visitors must be escorted in card access-controlled areas of facilities

E. CONFIDENTIAL AREA ACCESS

The following policy and procedure pertain to access to confidential UBH areas:

- All areas having sensitive information shall be physically restricted
- All individuals in these areas must wear an identification badge on their person so that both the picture and information on the badge are clearly visible to UBH personnel
- Restricted IT areas such as data centers, computer rooms, telephone closets, network router and hub rooms, voicemail system rooms, and similar areas having IT resources shall be restricted based upon functional business need
- Physical access to records having sensitive information, and storage of such records and data in locked facilities, storage areas, or containers shall be restricted
- Sensitive IT resources found in unsecured areas shall be secured to prevent physical tampering, damage, theft, or unauthorized physical access to sensitive information
- Appropriate facility entry controls shall limit and monitor physical access to information systems
- Video cameras and/or access control mechanisms shall monitor individual physical access to sensitive areas and this data shall be stored for at least three months, unless otherwise restricted by rule, regulation, statute, or law

Plant operations and information technology staff shall:

- Ensure visitors are escorted at all times in areas with sensitive information
- Restrict physical access to wireless access points, gateways, handheld devices, networking, communications hardware, and telecommunications lines
- Control physical and logical access to diagnostic and configuration ports
- Receive prior authorization before disposing, relocating, or transferring hardware, software, or data to any offsite premises

F. PHYSICAL SITE ACCESS

On-site physical access to sensitive or confidential areas for shall be controlled though a combination of the following mechanisms:

- Security based on individual job function
- Revocation of all facility access immediately upon termination and collection of keys, access/smart cards, and/or any other asset used to enter UBH facilities

Policies and procedures shall be established to ensure the secure use, asset management, and secure repurposing and disposal of equipment maintained and used outside the organization's premises.

G. CONTRACTOR REQUIREMENTS

External contractors shall comply with applicable laws and regulations regarding security and background checks when working in UBH facilities. For unclassified personnel, an appropriately cleared and technically knowledgeable staff member shall escort the individual to the area where facility maintenance is being performed and ensure that appropriate security procedures are followed.

- Any system access, initiation or termination shall be performed by the escort
- Keystroke monitoring shall be performed during access to the system
- Prior to maintenance, the information system is completely cleared, and all non-volatile data storage media shall be removed or physically disconnected and secured
- Maintenance personnel must not have visual or electronic access to any sensitive or confidential information contained on the system they are servicing
- Devices that display or output sensitive information in human-readable form shall be positioned to prevent unauthorized individuals from reading the information
- All personnel granted unescorted access to the physical area containing the information system shall have an appropriate security clearance

5. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of normal UBH operations. Examples of acceptable controls and procedures include:

- Access control procedures and processes
- Operational key-card access and premise control systems
- Operational video surveillance systems and demonstrated archival retrieval of data

6. Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

7. Distribution

This policy is to be distributed to all UBH staff.